2) Скільки взагалі існує чисел від 1 до N, які взаємно прості з заданим числом N?

Що таке взаємно прості числа? Взаємно прості числа – це числа, які не мають спільних дільників, окрім одиниці.

Тобто ми повинні обчислити потужність множини таких натуральних чисел, які належать цьому проміжку і не мають нетривіальних спільних дільників із числом N:

$\varphi(M) = \#\{x \in N \mid 1 \le x \le N, НД(x, N) = 1\}$

– функція Ойлера (Euler's totient(? Ніхто не знає) function)

Отже, як обчислювати це число?

По-перше, кожне натуральне число ми можемо розкласти на прості дільники. Можемо? В 5 класі ще повинні розкладати. Так?

Тобто я маю число $N = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$. Можу представити це число, де р-прості числа, а α – це певний степінь. Зветься це канонічний розклад числа.

Отже, якщо у вас число *x* має спільний дільник із числом *n,* то цей спільний дільник повинен ділитися або на p_1, або на p_2, або на p_3, або на p_t. *Це зрозуміло?*

(Якщо у вас $N = 2^{30}$, то які спільні дільники можуть бути в цього числа з іншими числами? 1, 2, $2^2, 2^3, ..., 2^{30}$; якщо буде $N = 2^{30} \cdot 3^{20}$: будуть усі степені 2-ки, усі степені 3-ки та їх множення; а спільний дільник «5» не буде, тому, що N не ділиться на 5; не може виникнути спільних дільників, окрім добутків степенів цих простих чисел).

Позначимо через A_i множину таких чисел, які лежать в інтервалі від 1 до N і поділяються на задане просте число p_i, яке ми взяли із розкладу нашого числа N: $A_i = \{x \in N \mid 1 \le x \le N, x \vdots p_i\}$.

Тоді що можна сказати про числа з множини A_i? Вони точно не є взаємно простими з N. Бо в них є спільний дільник, щонайменше ось цей $- p_i$.

Тому функція Ойлера для числа N: це мені потрібно взяти всі числа від 1 до N – і відняти всі числа, що входять до множин A_i. Тобто це буде: $\varphi = N - |A_1 \cup A_2 \cup \ldots \cup A_t|$. Зрозуміло?

А чому дорівнює потужність множини A_i? Множина A_i містить всі числа, що діляться на p_i-те (кожне p_i-те число буде ділитися на p_i). Тому: $|A_i| = \frac{N}{p_i}$.

А чому дорівнює потужність попарного перетину? $|A_i \cap A_j| =$

Перетин цих множин – це всі числа, які поділяються і на p_i і на p_j. Відповідно це буде кожне $p_i p_j$-те число: $|A_i \cap A_j| = \frac{N}{p_i p_j}$. Так?

Якщо в мене буде перетин по три – це всі числа, що поділяються на $p_i p_j p_k$: $|A_i \cap A_j \cap A_k| = \frac{N}{p_i p_j p_k}$.

І тоді, якщо ми застосуємо для того виразу: $\varphi = N - |A_1 \cup A_2 \cup \ldots \cup A_t|$, – формулу включень та виключень, то ми побачимо, що функція Ойлера: $\varphi(N) = N - \sum_{i=1}^{t} \frac{N}{p_i} + \sum_{1 \le i < j} \frac{N}{p_i p_j} - \sum_{1 \le i < j < k} \frac{N}{p_i p_j p_k} + \ldots + (-1)^t \frac{N}{p_i p_j \ldots p_t} =$ («+» сума по 4, «-» сума по 5, «+» сума по 6 і т.д. В кінці будемо мати ↑)

Якщо ми уважно подивимося на цей вираз, то можна побачити, що це розклад ось цього виразу: $= N\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\ldots\left(1 - \frac{1}{p_t}\right)$.

Цей факт я зараз залишаю без доведення, а ви вдома подивіться: доведіть методом математичної індукції.
Нарешті ми можемо перейти до нової теми.
Сьогодні ми повинні розглянути методи конструювання складних множин, коли у вас є певні прості.
Першою такою складною множиною є так званий булеан.
Булеаном множини А ми називаємо **множину всіх її підмножин**.
Традиційне позначення для булеана: 2^A. Але я підкреслюю: це не 2 піднести до степеня множина А, – тобто 2^A – це не операція, це символ, що означає булеан!!! Це лише позначення для булеана.
Є альтернативні позначення для булеана: $\mathrm{P}(A)$ або $B(A)$.
Чому саме такий символ (2^A) зараз покажу.
Ну і формальне визначення: $2^A = \{B \mid \mathrm{B} \subseteq \mathrm{A}\}$ – булеан це є множини, які є підмножинами множини А.
Які є **очевидні властивості булеана**?
$\varnothing \in 2^{\mathrm{A}}$ – пуста множина є елементом будь-якого булеану (бо порожня множина завжди є множиною будь-якої множини);
Наша вихідна множина також завжди є власною підмножиною, тому вона завжди належить нашому булеану: $A \in 2^A$.
Тобто ці дві властивості є тут (які виконуються для будь-яких множин).
А скільки взагалі підмножин буде в нашій множині?
Якщо наша множина А скінченна, то в мене є теорема.
Теорема (про потужність булеана): **якщо** множина **А** є **скінченною** і містить n елементів, то її булеан містить 2^n елементів. Тобто потужність булеану обчислюється за допомогою такого виразу: $\left|2^A\right| = 2^{|A|}$. Або: $|A| = \mathrm{n} \Rightarrow \left|2^{\mathrm{A}}\right| = 2^n$. Що одне і те ж саме.
Якщо в мене множина А складається з 1 елемента. То скільки в неї підмножин? 2. Які? Ø та сама множина А.
Якщо в мене множина А складається з 2 елементів: $\mathrm{A} = \{\mathrm{a}, \mathrm{b}\}$, то в мене є: $2^A = \{\varnothing, \{\mathrm{a}\}, \{b\}, \{a, b\}\}$. Можна перевірити для 3-4 елементів множини. І ми бачимо, що твердження здається коректним. Добре. Нам це потрібно доводити. Як ми це будемо доводити? Методом математичної індукції.
Але це буде один з його способів, який ми сьогодні розглянемо.
Доведення
(1-ий спосіб).
Отже, доводимо методом математичної індукції. З чого починаємо? З бази.
Яку беремо базу? $\mathrm{n} = 0$.
У нас в множині може бути 0 елементів, але менше 0 бути не може.
(математична індукція – ми починаємо з найменшого числа, яке у нас є).
Отже, якщо $\mathrm{n} = 0$: $2^{\varnothing}$ Як виглядає булеан порожньої множини? $2^{\varnothing} = \{\varnothing\}$ – це множина, яка містить один елемент – Ø (порожню множину).
Потужність такого булеану: $\left|2^{\varnothing}\right| = 1 = 2^0$, бо це множина, що містить 1 елемент. А $1 = 2^0$.
База в нас сходиться.
Ви вже не плутаєте порожню множину і множину, що містить порожню множину? Так? ☺ Це різні речі.
Припустимо, що твердження нашої теореми стверджується для всіх множин, потужності n. То що буде із множиною потужності $\mathrm{n}+1$?
Розглянемо множину В: $B = \{b_1, b_2, \ldots, b_n, b_{n+1}\}$. Очевидно, що будь-яка підмножина множини В містить елемент з номером $\mathrm{n}+1$ або його не містить. Очевидно?

І це задає нам розбиття всіх підмножин на 2 незалежні підкласи. Клас не може містити і не містити елемент одночасно. І будь-яка множина може бути описана в такий спосіб.
Тобто мені можна окремо обчислити кількість підмножин, що не містять b_{n+1} і окремо обчислити кількість підмножин, що містять b_{n+1}-ше і додати ці два числа.
Це зрозуміло?
Отже, скільки підмножин у мене не містять b_{n+1}?
Якщо у вас підмножина не містить b_{n+1}, то вона є підмножиною множини від b_1 – до b_n. А це є множина потужності n.
За припущенням індукції кількість таких підмножин буде 2^n.
Тобто, якщо у мене є підмножина $B_1 \subseteq B$ і $b_{n+1} \notin B_1$, то кількість таких підмножин дорівнює 2^n - за припущенням індукції: $\#B_1 = 2^n$ (бо насправді $B_1 \subseteq \{b_1,...,b_n\}$). *Згодні? Добре.*
Якщо у мене $B_2 \subseteq B$ і $b_{n+1} \in B_2$. Давайте візьмемо цей елемент $n+1$-ий і вилучимо його. Тобто множина B_2 – з якої вилучили елемент b_{n+1} – вона є підмножиною множини від b_1 – до b_n: $B_2 \setminus \{b_{n+1}\} \subseteq \{b_1...b_n\}$. *Так?*
Тому я зразу можу сказати скільки множин B_2 існує: $\#B_2 = 2^n$ – за припущенням індукції. Тобто всі множини B_2 можуть бути одержані таким шляхом. Берете підмножину цієї множини – додаєте до неї елемент b_{n+1}.
І відповідно загальна кількість підмножин $\left|2^n\right| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$. Чи є у вас питання в тому, що я тут будувала?
Знову ж таки: всі підмножини, які у мене тут є я розбиваю на 2 незалежні класи, тобто я певну множину віднести до певного класу – і ці множини не перетинаються, тобто не має множини, яка належить двом класам одночасно. Тут це буде диз'юнктне об'єднання. Обчислюю потужність кожного класу. Як? За припущенням. Тобто я зводжу наше обчислення – то того твердження, яке вже є коректним для нас. І обчислюю загальну кількість. І виявляється, що якщо припущення індукції вірне для n, то воно буде справедливе для довільної множини потужності $n+1$.
Звідси індукційний перехід дає нам справедливість теореми для довільної множини, потужності n.
(2 спосіб)
Ви можете запитати мене: чому я даю два способи доведення одного і того ж самого твердження? Чи вам отого не достатньо? Взагалі то достатньо, але для того, щоб ви бачили, як це можна робити. Тому, що в деяких випадках працює ось таке, а в деяких випадках ось таке не працює. Працює щось інше. Наприклад те, що буду розповідати зараз.
Зараз ми доведемо практично методом комбінаторного обрахунку. Хто в школі полюбляв комбінаторику? ☺ Вау! Є такі люди? ☺
$A = \{a_1, a_2,..., a_n\}$ – ось в мене множина з n-елементів. Ось ці елементи в мене є і пронумеровані. Так? Ось в мене є певна підмножина множини A: $B \subseteq A$. Давайте я навпроти елемента буду ставити 1, якщо він належить цій множині (B), 0 – якщо не належить. Тоді я цю підмножину B можу представити у вигляді: 0 1 0 1 … 1 – певного бітового вектора («одиничкі» стоять навпроти тих елементів, які належать, «нулики» – навпроти тих, які не належать).
Зрозуміло, що кожну підмножину можна так подати.
Зрозуміло й інше: кожний бітовий вектор довжини n задає певну підмножину. Так? Більш того: 2 різні вектори задають різні підмножини. А дві різні підмножини задають два різні вектори. Чому? Якщо підмножини різні, то там є елемент, що одній множині належить, а іншій не належить. Інакше вони співпадають по всіх елементах.

Ось наприклад:

$B \subseteq A$ 0 1 0 1 … 1

$C \subseteq A$ $\underbrace{0\,0\,1\,1\,\ldots\,1}_{n} \Rightarrow$

Ось по 2-му елементу ці дві підмножини (B і C) будуть відрізнятися.

Тобто співставлення бітового вектора нашим підмножинам – воно однозначне: одній підмножині – один бітовий вектор.

Тому кількість підмножин може бути лише такою, як кількість n-бітних векторів. А скільки у мене існує n-бітних векторів? В мене є n-бітів, кожен біт приймає значення 0 або 1 (кожен елемент може мати 2 варіанти). І треба все перемножати, оскільки ми одночасно обираємо ці варіанти.

$\Rightarrow 2^n$ бітових векторів.

А якщо векторів у мене 2^n, то і підмножин буде 2^n.

Десь через місяць ми ось цей принцип доведемо формально. Тобто дві множини мають однакову кількість елементів, якщо можна побудувати між цими елементами взаємно однозначне представлення – бієктивну функцію.

А тепер подивіться скільки місця в попередньому способі, скільки в цьому (скільки різних тверджень я доводила там, скільки тут). *Я дуже полюбляю це доведення ☺.*

Чи є у вас питання?

Наступна конструкція, яку ми будемо розглядати – покриття множини А.

Покриття множини А.

Покриття множини А – це така система множин, об'єднання яких накриває всю множину А.

Тобто елементами покриття є підмножини множини А:

$\Delta \subseteq 2^A$ (покриття можна позначати великою грецькою літерою Δ)

$\Delta = \{T_1, T_2, ..., T_t\}$

Ці елементи задовольняють двом умовам:

1) всі елементи покриття є не порожніми множинами $T \neq \varnothing$;

2) а їх об'єднання дає всю множину А: $\bigcup_{i=1}^{t} T_i = A$.

Тобто, якщо у вас є множина А, то тут є якась множина T_1, T_2, T_3, T_4 і вони так «лап, лап, лап» – і усю множину А накрили (рис. 1).

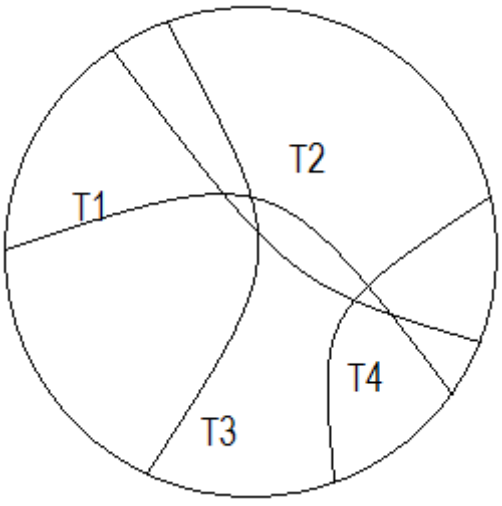


Рис. 1

Кожен елемент з множини А буде належати якійсь з множин Т, можливо, неподільній. В топології, ще в якихось розділах математики це поняття розглядають в більш широкому сенсі, де це може бути система довільних, в тому числі таких, які виходять за межі множини А. Але в нас важливо, щоб це були саме підмножини множини А.

(Чому? Через 3 лекції ми будемо доводити теорему про фактор підмножин)

а) частковий випадок покриття: **розбиття множини А**.

Розбиттям множини А ми називаємо таку систему множин Π (це велика грецька літера «пі»): $\Pi \subseteq 2^A$, $\Pi = \{T_1,...,T_k\}$.

1) Ця система множин, по-перше, є покриттям.

2) і по друге: для всіх $i \neq j$ ці множини не перетинаються між собою: $i \neq j \;\; T_i \cap T_j = \varnothing$.

Тобто, якщо в покритті ці елементи могли перетинатися і кожен елемент міг належати декільком частинам покриття, то в розбитті кожен елемент належить рівно одній частині розбиття.

Якщо ми покриття схематично зображаємо так (рис. 1), то розбиття (рис. 2): ☺ берете тарілку – розбиваєте, – і те, що трапилось це і є розбиття.

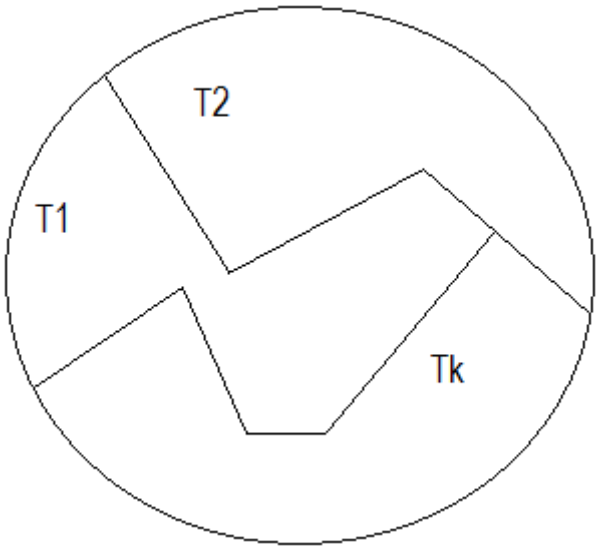


Рис. 2

Зрозумілі ці поняття?

Приклади:

1) скажімо, беремо множину натуральних чисел N. В мене є парні натуральні числа, в мене є непарні натуральні числа.

Чи може число бути одночасно і парним і непарним? Ні, не може.

Чи може бути число, що не є парним, ні непарним? Ні.

Тому, якщо я візьму всі парні числа $(2N)$ і всі непарні числа $(2N-1)$: $N = 2N \coprod (2N-1)$, – то вони задають розбиття множини натуральних чисел.

Тобто, ось ця система: $\Pi = \{2N,\ 2N\text{-}1\}$ – це розбиття.

Взагалі кажучи, якщо Π – це розбиття, то я завжди можу написати, що в мене множина $A = T_1 \coprod T_2 \coprod \ldots \coprod T_k$ – ось цих всіх частин.

І починаючи з цього моменту я перестаю казати «диз'юнктне об'єднання» – я буду казати лише «розбиття». Тому, що це більш зрозуміло.

Це все зрозуміло? Добре.

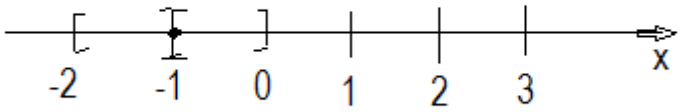
2) Знову беремо натуральні числа. Є прості натуральні числа, є складені натуральні числа. Чи може бути число одночасно простим і складеним? Ні, не може.

Тому я можу сказати, що довжина натуральних чисел – це прості числа і складені числа: $N = \text{прості} \coprod \text{складені}$. Так? Всі згодні? Якщо так, то «2 бали» всім! ☺

А чи є у нас натуральні числа, які не є ні простими, ні складеними? Одиничка (1) – вона не є простим числом, бо просте число має два різні дільники: 1 і саме себе; а 1 не має двох різних дільників. $N = \text{прості} \cup \text{складені} \cup \{1\}$ – а ось тепер це буде розбиття.У нас всі натуральні числа входять в якусь з цих множин і лише вони.
Зрозуміло? Добре.

3) Нехай множина A_0 – це множина всіх цілих чисел, що діляться на 3: $A_0 = \{3k \mid k \in Z\}$, множина A_1 – це всі числа, що дають при діленні на 3 остачу 1: $A_1 = \{3k+1 \mid k \in Z\}$, ну і множина A_2 – це всі числа, що дають при діленні на 3 остачу 2: $A_2 = \{3k+2 \mid k \in Z\}$. Чи можуть у мене бути ще якісь остачі? При діленні на 3 остача може бути лише 0, 1 або 2. От вам 0, от вам 1, от вам 2. Тоді система множин A_0, A_1, A_2 – це що? Розбиття. Розбиття чого? Множини цілих чисел. Ви не можете казати просто «розбиття», бо ви повинні прив'язатися до вихідної множини – яку ви саме розбиваєте. Тобто у мене $\{A_0, A_1, A_2\}$ – це розбиття множини цілих чисел.

4) Розглянемо систему відрізків числової осі (одиничні відрізки: від цілого числа k – до цілого числа $k+1$):
$C_1 = \{[k, k+1] \mid k \in Z\}$.
Ці відрізки перетинаються. То що таке є система C_1? C_1 – це покриття всіх дійсних чисел – R .
У вас є відрізок $[-2,-1]$, у вас є відрізок $[-1,0]$ і вони перетинаються в точці -1 (рис. 3). Тобто число -1 належить одночасно двом відрізкам. Відрізки $[-1,0]$ і $[0,1]$ теж перетинаються, $[0,1]$ і $[1,2]$ теж перетинаються, – але в сукупності вони перетинають усю числову вісь. Тому система C_1 – це є покриття множини дійсних чисел.



Добре. Розглянемо систему C_2 – напівінтервалів одиничної довжини: $C_2 = \{[k, k+1) \mid k \in Z\}$. Що таке система C_2? Це вже розбиття. Бо ці точки, що належать двом відрізкам, за рахунок того, що я їх вилучаю зліва відрізків, – вони належать лише одній з цих множин. Отже, C_2 – це розбиття R .
І нарешті система $C_3 = \{(k, k+1) \mid k \in Z\}$ інтервалів на числовій осі. Що таке C_3? Ми не можемо класифікувати цю систему множини. Воно не є покриттям, оскільки цілі точки не належать жодному з цих інтервалів. Так? Тобто всі ці множини не порожні, але їх об'єднання не дає множину дійсних чисел. Тому це не є покриттям, – і відповідно не є розбиттям. Ось. Все зрозуміло? Добре. Переходимо далі.
Наступна операція над множинами, яка конструює множину складного вигляду – декартовий добуток двох множин.